Arkansas SHARE RFI Response

From ProSys - Vendor for CA and Unityware

Mike Morris
ProSys
Sales Manager
870.335.0356
mmorris@ProSysis.com

Don Pennington
Unityware
don.pennington@unityware.com
501.258.3667

John Morgan
CA
Solution Strategist
225.202.5881
john.morgan@ca.com

May 7, 2010

May 7, 2010

Arkansas State Health Alliance for Records Exchange (SHARE)
1401 West Capitol
Suite 300, Victory Building
Little Rock, AR 72201

Dear Members of the Committee,

We are excited to respond to the Request for Information for the Arkansas Health Information Network. We are pleased to present a complete and comprehensive solution, and we appreciate your consideration of this proposal.

When reviewing the solution being presented in this document three sayings seemed to sum up the theme very well.

2. "Begin with the end in mind", Steven R. Covey (*The Seven Habits of Highly Effective People*)
3. "The definition of insanity is doing the same thing over and over and expecting different results", Albert Einstein
4. "Keep your feet on the ground and keep reaching for the stars", Casey Kasem

Firstly (Quote 1), the solution being presented here is scalable. It can work in a small setting, and in fact currently is. Yet it can easily scale out to cover every provider of health care, every consumer, every payer, and every agency. The initial investment is protected, as are all future layers upon the system. This system was not designed to win one contract, but to eventually link ALL medical records.

Secondly (Quote 2), the solution presented is not a repackaging of the solutions that have failed in the past. It certainly is standards based, and relies on proven security methods, development methods, and services through organizations and individuals with great track records of success. However, it also centers around a revolutionary new 'Interface-less' Interfacing Technology that a large, international, independent IT research firm has declared to, *"Create its own category of computer technology."* In order to escape from the countless failures of the past with these types of medical records exchange systems we must go down a new road. This document presents a solution with this fact in mind.

Finally (Quote 3), Do not be bound with the limitations of the past. Don't allow past failures, due to poor technologies, to cause the bar to be set too low. If the expectations are set very small, then the end result will be small and lacking. Set the bar high, and reach for the stars, but remain grounded in reality by seeing and experiencing what is now available before investing. Using this solution, Arkansas doesn't have to 'eat the whole elephant in one bite.' We can prove out the solution, over time, and greatly minimize the risk of waste and failure. As the system grows, nothing will have to be abandoned in favor of a new approach. Reach high, but do so with low risk.

Thank you again for your time, and your interest in our proposal. We look forward to working together to serve the citizens of Arkansas with a secure, robust, and cost effective solution.

Sincerely,

ProSys, Unityware, and CA

Table of Contents

1. Summary of Solution

This solution is a comprehensive one designed to automate the HIE Process from end to end in a way that is accurate, responsive, reliable, and secure. The solution is called the State And smaller Geography Electronic Medical Records System (SAGEMR). This SAGEMR System is being presented by three partner companies, Prosys Information Systems, CA Inc, and Unityware.

These three solution providers have collaborated to offer a solution to health care that is the first of its kind. With this solution a patient can seek treatment anywhere and their complete medical records can follow them. Providers will know their patients' histories, their current medications, their allergies, etc... Citizens will be able to safely access their own records and manage them, much as they do their banking records or their credit report. States and research groups will be able to mine, real time data, for trends in diseases and conditions without threatening the privacy of any patient. Payers will be able to have eligibility verified, and know that they are not paying for repetitive testing that is unnecessarily scheduled. Doctors and hospitals will be able to access this ubiquitous information without having to replace existing expensive systems with new expensive systems in anticipation of improved access to the same data - and all of this will be accomplished securely, accurately, and quickly.

The challenges facing the medical community, in terms of exchanging needed information, are in sharp focus while the solutions offered from the health care information technology mainstream remain more than a little fuzzy. While large amounts of valuable data exist within existing systems, the systems have been so competitively designed to isolate the data that getting actionable information from them is arduous at best and dangerous at worst. Correcting even a small amount of this problem is now an enormous manual chore and there is not enough time nor are there enough bodies available to do this work by hand. A real solution to these problems is one that employs real end to end automation.

We cannot stress enough that: **the data is already there!** Data resides within various parts of the Hospitals, the Pharmacies, the Insurance Providers, Medicare records, Medicaid records, Laboratories, and perhaps most importantly the Clinics staffed by Primary Care Physicians and Specialists. But the traditional methods for sharing this data between traditional health care software systems usually result in such long and expensive programming projects that most give up and replace perfectly good systems with new and larger systems with even larger price tags or just give up on the endeavor altogether.

Even if money were no object, the training burden alone caused by installing new systems across the United States would prevent success. Currently, the American Recovery and Reinvestment Act (ARRA) is mandating “Meaningful Use” of EMR. Traditional health care system vendors are rushing to create and install new systems that can share data intra-system. However, there is no mandate for these vendors to work together to share information inter-system. An analogy might be helpful.

> Think with me hypothetically. It is one day determined (for some strange reason....its just an analogy) that all cars, trucks, and other motor vehicles on the streets be shared between all authorized drivers. Authorization could mean a friend borrowing a friend's car or a police officer being able to easily jump in any police car in order to fight crime. This authorization, for example, could be in the form of a fingerprint system. A mandate goes out to all the companies making vehicles that they must now standardize on one common platform, within **their** company. Ford Motor Company goes to work changing all their new cars, and soon all new Ford models can be exchanged between new Ford drivers. A Toyota owner can drive any new Toyota, etc... However, no Lexus owner is any closer to sharing a Cadillac than he was

before.

What about the millions of vehicles that are already on the roads? Can we afford to scrap all of them? Even if we did that still wouldn't solve the problem. We still wouldn't reach the goal of universal access for vehicles.

The answer, therefore, is not to change the vehicles. The answer is to **change the KEYS**. What if, instead of changing all the vehicles, someone came up with a revolutionary new type of key? The cars could be the same, but the key would miraculously transform to fit any vehicle. The key could also integrate with the security authorization system and authenticate the drivers using fingerprints. A Buick driver would be able to get in and drive any Hyundai, Dodge, Mercedes, or antique Studebaker. For that matter, they could also use this new key on motorcycles, fire engines, 18-wheel diesels, or dump trucks. This new type of amorphous key would be able to solve the problem of making all vehicles sharable, but would also be far less costly and time consuming than changing the vehicles themselves.

The main point in this analogy is that it is foolish to even think about changing or completely scrapping the most expensive components, the vehicles, if instead we could simply create a universal skeleton key that would serve as a secure universal connector. Expecting competing companies to agree on a standard, and having to scrap the millions of vehicles on the road is a clear recipe for failure.

The point of this story is this: *the status quo simply won't do*. We cannot afford to change all the systems currently in place. It is too burdensome, too costly, to time consuming, and would require too much retraining. With that in mind, we introduce the center point of the SAGEMR System. It is a revolutionary new piece of computer technology, which is already working at a hospital in the State of Arkansas. The Unityware solution is an extension of patented technology that an IDC report labeled, "a revolution." Unityware has invented, according to a leading international and independent IT research firm: "a new category of computer technology". Unityware provides the amorphous key which reaches into existing and new software systems by any source and retrieves the data from any of these systems. Unityware can bring together any number of disparate systems WITHOUT a traditional software interface. The old limitations of interfacing are blown away. The SAGEMR system can be installed faster, with more accuracy, and more economically at a fraction of the cost and time.

Also, once connected to Unityware, traditional systems can be changed, upgraded, or removed altogether without destabilizing the community of connected systems. Unityware, in a unique sense, actually unifies systems by first insulating them with what is called a contextual buffer. Therefore, the traditionally fragility associated with connected systems disappears. Systems, within the super system, can change multiple times without cascading failures throughout the systems. This technology is new, but it is real and demonstrable in a hospital environment as well as an entire community.

Using the Unityware technology to bring together data from disparate sources the SAGEMR System recognizes the patient. We accomplish the recognition piece using a proprietary knowledge-base based matching that can increase matching accuracy rates by at least 10% over traditional string based matching. Any good matching system can 'recognize' that Elizabeth Jones at 123 Main Street, Orlando FL is the same person as Beth Jones at 123 Main Street, Orlando FL. However, using a multi-billion row database of historical knowledge we can know that she is the same person as Beth Davis (She got married) at 456 Oak Lane (She moved).

The SAGEMR System then creates a Master Patient Index (MPI). The MPI represents a complete and accurate view of all the data available for that one person. While all systems with a patient's data are available and on-line the MPI will be real-time current.

However, what if systems that feed this data are not on-line at the moment? What if a doctor turns off his/her EMR server? Then the SAGEMR System will rely on a backup of that source of data housed in what is called a virtual clinic. When the virtual clinic data is relied upon due to such an outage the information presented to the providing doctors is indicated as having come from an alternative source and will be persistently recorded as such for malpractice liability purposes. Every translation the system processes is recorded and time stamped and kept indefinitely.

Whenever the subject of medical records comes up, the subject of security is not far behind. The SAGEMR System is built from the ground up with accuracy and security as the cornerstone of all design. Multiple layers of security are created from beginning to end by native design and augmented with proven and state of the art security products from CA Inc. CA is the world's leading company in IT security, securing clients throughout the banking industry, the government, transportation, and beyond. Of course, CA is no stranger to the health care industry as well, securing numerous health care organizations and winning awards as the provider of choice among various health care entities. With the SAGEMR System nothing is left to chance.

Robust reporting will also be available. This system allows for redaction of personally identifiable information (Name, Address, SS#, etc...) in order to run aggregate reports in real time. With this system, for example, the ability to quickly and easily access the number of H1N1 cases in a particular set of counties where the patient is over 35 and is a female can be generated. The options here are almost limitless.

In the end, the health records belong to the patient. These citizens/patients should be given access to their own records in a safe and secure way. This is similar to logging on and seeing a person's credit score or their on-line banking records. The SAGEMR System has this functionality built in.

Finally, the system must be effectively installed, supported, and maintained. That is where Prosys Corporation comes in. As an accomplished systems integration reseller, Prosys brings the implementation and project management expertise for Unityware/CA projects to the health care market.

As you can see this solution presents a complete solution that utilizes things that have been proven to work in the past, while bringing in new technologies to avoid past failures.

2. Overall System Design

2.1 Basic System Architecture

The overall system design at its basic level is laid out in the diagram below.

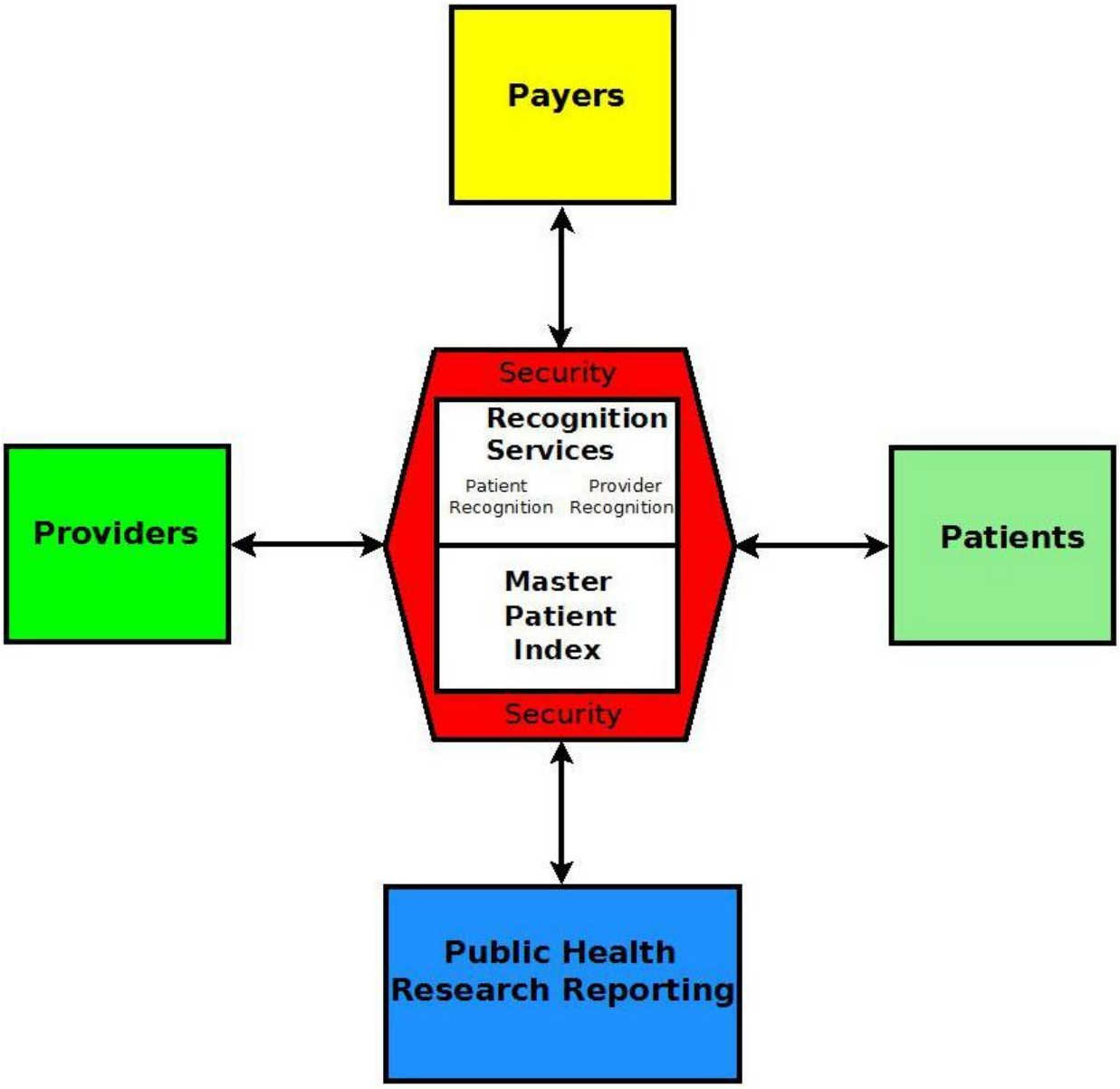


Figure 2-1

This base, high-level, design shows that all entities needing connection, will be connected to the super system. However, within the various areas this document will further break down the individual areas in subsequent sections.

2.2 Parallel Design and Build

On May 10th, 1869 a ceremony was conducted in Promontory Summit Utah. At the conclusion of this ceremony, a one word telegraph message was sent out to both the East Coasts and West Coast of the United states, and spontaneous celebrations erupted across the entire country to honor this historic event. The one word message that was sent was the word 'Done'. What had been done was the pounding of the last spikes into the last sections of rail uniting the United States of America from coast to coast. Until that time, a trip from the Atlantic to the Pacific or vise versa took over six months. The completion of the trans-continental railroad lowered the time to one week. America took a giant leap forward, and was changed forever.

As great an event as that was, one question must be asked by the casual observer. Why was the last section of rail completed in Utah? Utah seems an unlikely place for this historic event to take place. Utah is thousands of miles from either the West or the East coasts. Did they start laying rail from East to West, skip over that short section, and then come back to it at the end? Did the reverse occur? Why would a famous 'Coast to Coast' railroad not be finished when it got to the coasts themselves?

Of course, the answer is a logical one. Instead of working East to West or West to East they started on BOTH sides and worked their way to the middle. In fact, the East Coast did not have as far to go, because they already had a somewhat robust rail service as far west as Iowa. They built upon what they had so as not to waste their previous investments as well as starting on new territory in order to bring it all together. Meeting in the middle saved a tremendous amount of time, money, and labor. It protected previous investments and hurried completion exponentially. It should also be noticed that both crews built their rail to the exact same specifications. Had they met in Utah and one of the crews had been building their rail even a few inches wider than the other, the tracks would have been useless.

With this in mind the SAGE-MR System is designed to be built and implemented from both sides of the problem, and to meet in the middle with a COMPLETE solution. By 'beginning with the end in mind' and working the problem from multiple angles, the SAGE-MR System will protect all investments, lower costs, lower risks, provide greater functionalities, and speed time to implementation. In fact, as with the railroad example earlier we have already started implementation of part of the complete solution in communities around the state of Arkansas.

2.3 Parallel Phase A – Inter-Hospital Records Transfer

In talking to numerous experts from numerous states throughout the country it is common to find that people tend to think about the providers connections to the state HIE as looking something like Figure 2-1 shown below.

What is shown is central HIE tied to various hospitals, thereby tying them together and allowing them to share records. While this is certainly correct and necessary design, we believe that it will lead to ultimate failure if this is the **first and only** path taken.

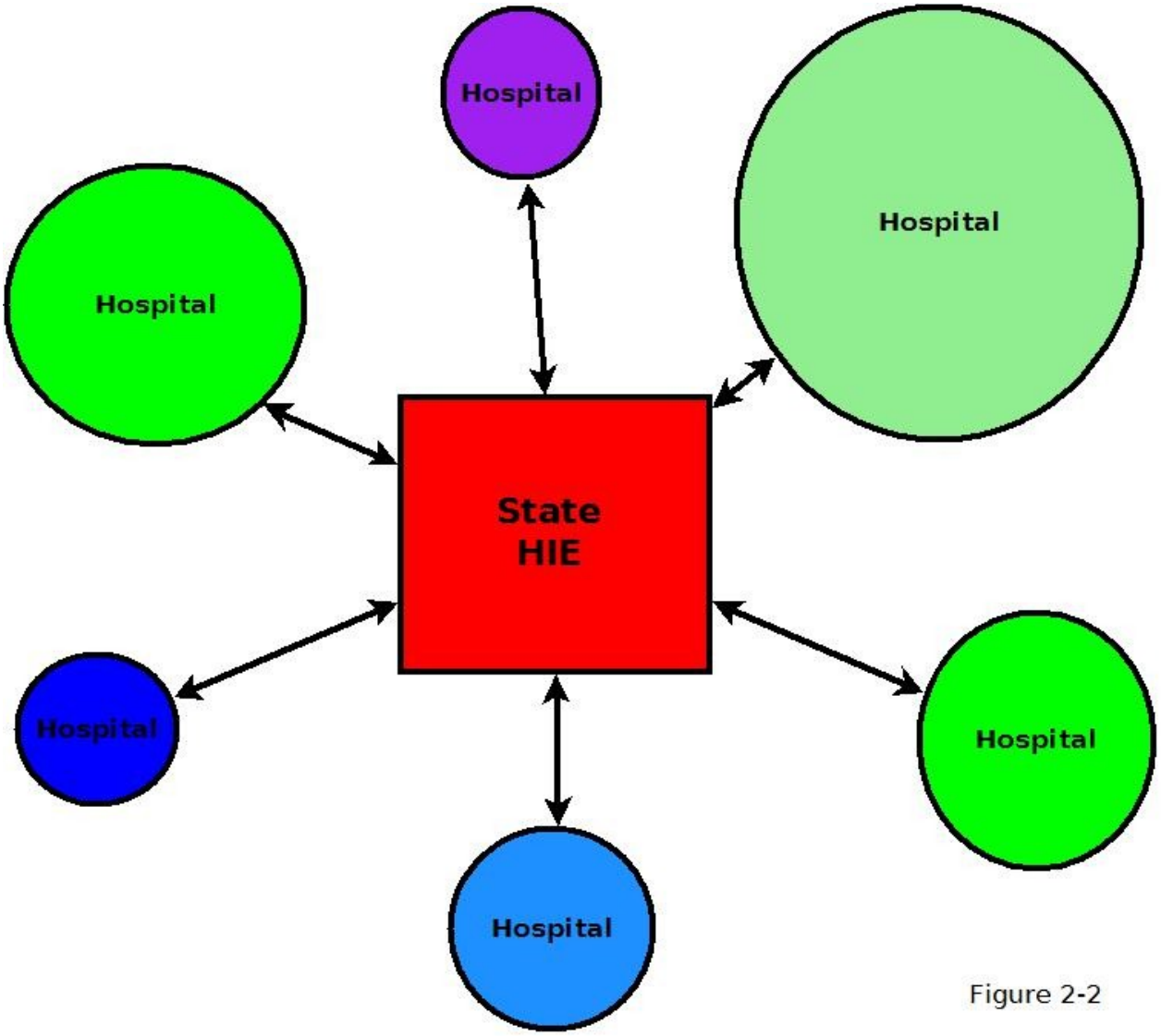


Figure 2-2

Why would this not be adopted by the hospitals if it could be shown to work ('work' meaning to aggregate disparate sources of data from the hospitals to recognize a patient and create an MPI quickly and securely)?

Why it might fail is because we would be asking all hospitals to get on board with a system that would provide very little value to a large percentage of them while putting them at, what they perceive, great risk and effort. Even if all hospitals could be linked together, that would not allow access to the vast majority of patient information because that information is not in hospitals. It is in clinics.

The following objections from hospital administrators and IT people would be common.

- “We're just a small hospital. We don't transfer that many patients and when we do we just fax the information over.”

- “We are small so we never get anyone sent to use so you would only be providing us half the value while making it easier to lose our patients to larger hospitals.”
- “This is great if I have a patient that I need to transfer in or out to another hospital, but what about a patient who has never been in the hospital and comes in complaining of chest pains or has been in an accident. His records are at his doctor's office. This won't help me there.”
- “I just don't see the value and there is no way we are letting you make a connection to our Cerner/McKesson/CPSI/Medatech/etc... system and risk messing things up. The risk is too great for the limited value we are seeing in this.”

Don't misunderstand, the SAGE-MR System certainly is built to connect hospitals, but it must provide more value than only that and deliver it up front if possible. This section will answer, “How?”

2.4 Parallel Phase B – Inter-Geography Providers Transfer

The key here is connecting local hospitals with their community of physicians and possibly local labs and/or pharmacies. Most medical information is stored in the clinics. This is where we need to be connecting to get the most bang for the buck and to lower the risk of failure. That model looks something like figure 2-3.

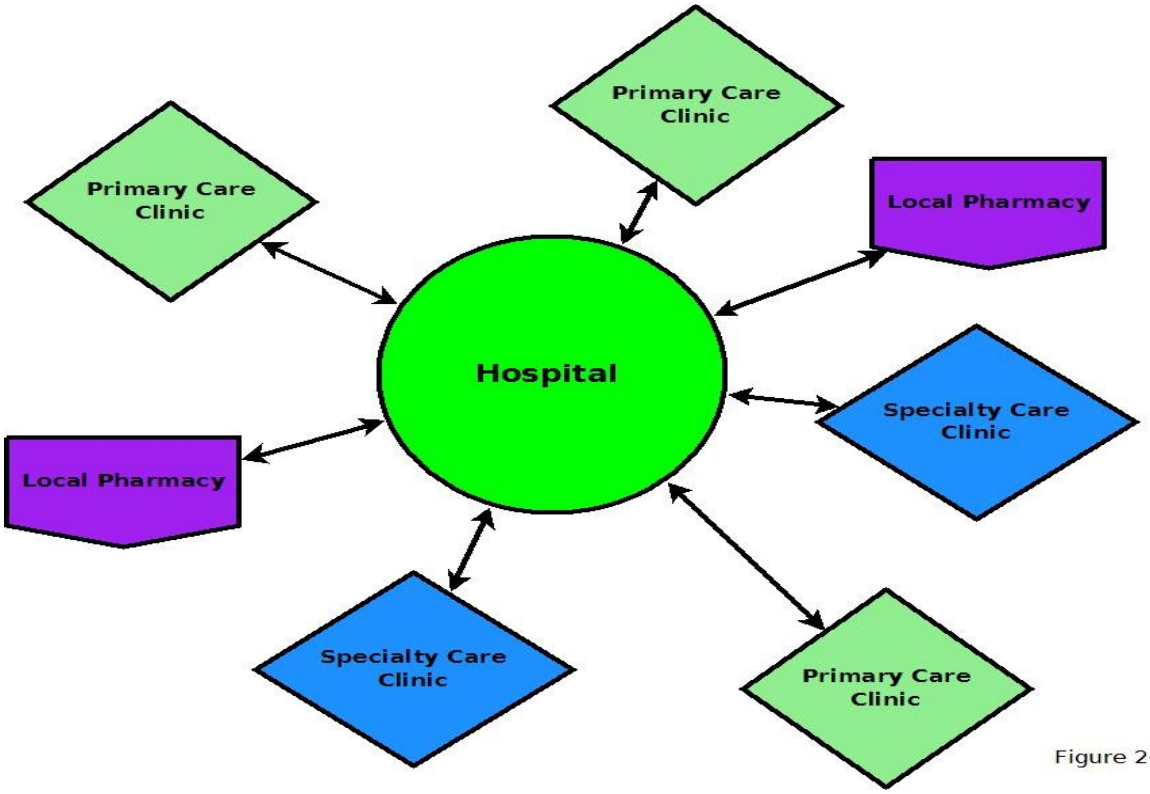


Figure 2-4

This parallel creation brings a lot to the table. It allows access to the heart of medical records by the super system and it contains a number of business advantages to the hospitals, especially since a vast majority of the patients visit and stay within their local communities. These advantages include;

- The ability to better serve their community of physicians by linking their data to the hospital's.
- The ability to better serve their community of physicians by allowing referrals between those doctors.
- The ability to better create and support a hospital's Hospitalist doctor program.
- The ability to better attract and retain patients to their community hospital through better care.
- Lower costs through efficiencies.
- The ability to detect 'drug shoppers' and other fraud in a community and beyond.
- Computerized Provider Order Entry (CPOE) for inpatient and outpatient testing.
- Less paperwork and faxing by the clinics and the hospital.
- Predictive community-wide work-flows (chains of authority)
- Physician Documentation
- Radiology Images
- Secure community Communications

However, as great as these advantages are there are still significant gaps if the individual hospitals are not connected. Therefore, it becomes obvious that Parallel Phase A and Parallel Phase B must be undertaken together in order to meet in the middle and create something truly worthwhile.

2.5 The Power of Two! - Phases A & B Combined

By working from both directions and meeting together in the middle the State of Arkansas can have a very robust and highly valuable HIE system that can become the model for America and beyond.

Already we have seen the limitations of one vs. the other. Why not go after both in such a way as to increase the chances of success and negate the risks of failure?

As stated earlier, Unityware and ProSys are already working within the State of Arkansas proving and installing community-wide EMR systems. These systems are live and demonstrable today. They bring the values listed in Section 2.4, and they are a microcosm of what a statewide system would look like.

The solutions already in place can be thought of as the train track being laid East to West. Now it is time to marry that to the tracks (the State Level) being laid West to East. One thing that the SAGE-MR System will not claim is that we are the only possible provider of the community system. We are definitely one of the possible solutions, but if individual hospitals wish to use other vendors or design and build their own home-grown solution then the SAGE-MR system can connect to it if they meet minimum standards. Our approach is very flexible on the community level should the SAGE-MR system be adopted on the state level.

Figure 2.5 gives a graphical representation of how the complete system would look:

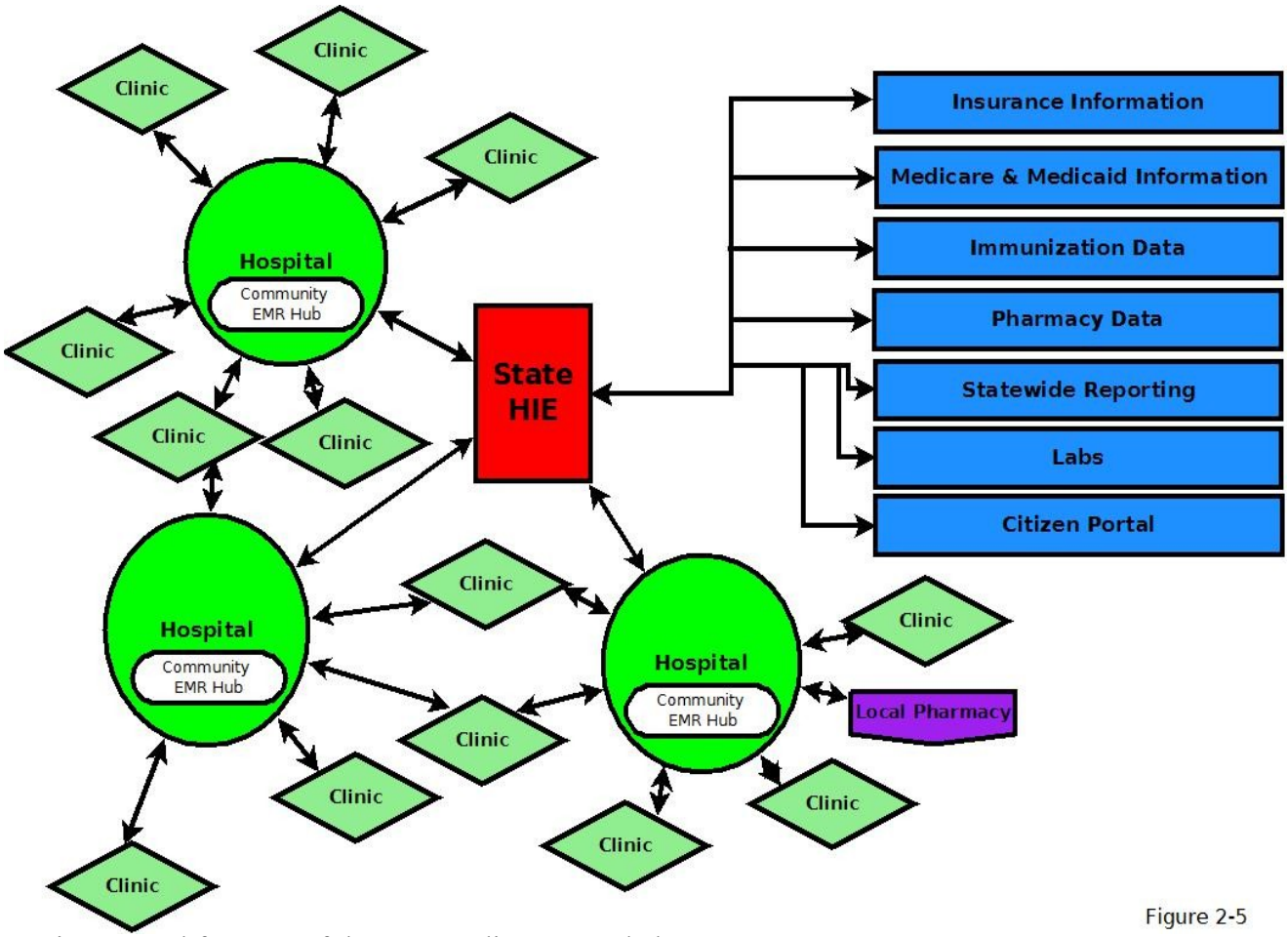


Figure 2-5

Notice several features of the system diagrammed above:

- The communities are connected from hospital to clinic and host their own mini-version of the HIE.
- Clinics can be connected to just one or multiple hospitals.
- Moreover, the clinics can be connected to one another for referrals.
- All the hospitals are connected by the central State HIE.
- The state HIE is the single point of entry for very valuable information from:
    - Insurance
    - Medicare and Medicaid
    - Pharmacy Chain Data
    - Immunization Records

- Laboratories
- Statewide Reporting
- Citizen Portal

Given the tremendous value of that information flowing into the State HIE it makes the idea of connecting to it much more attractive for an individual hospital.

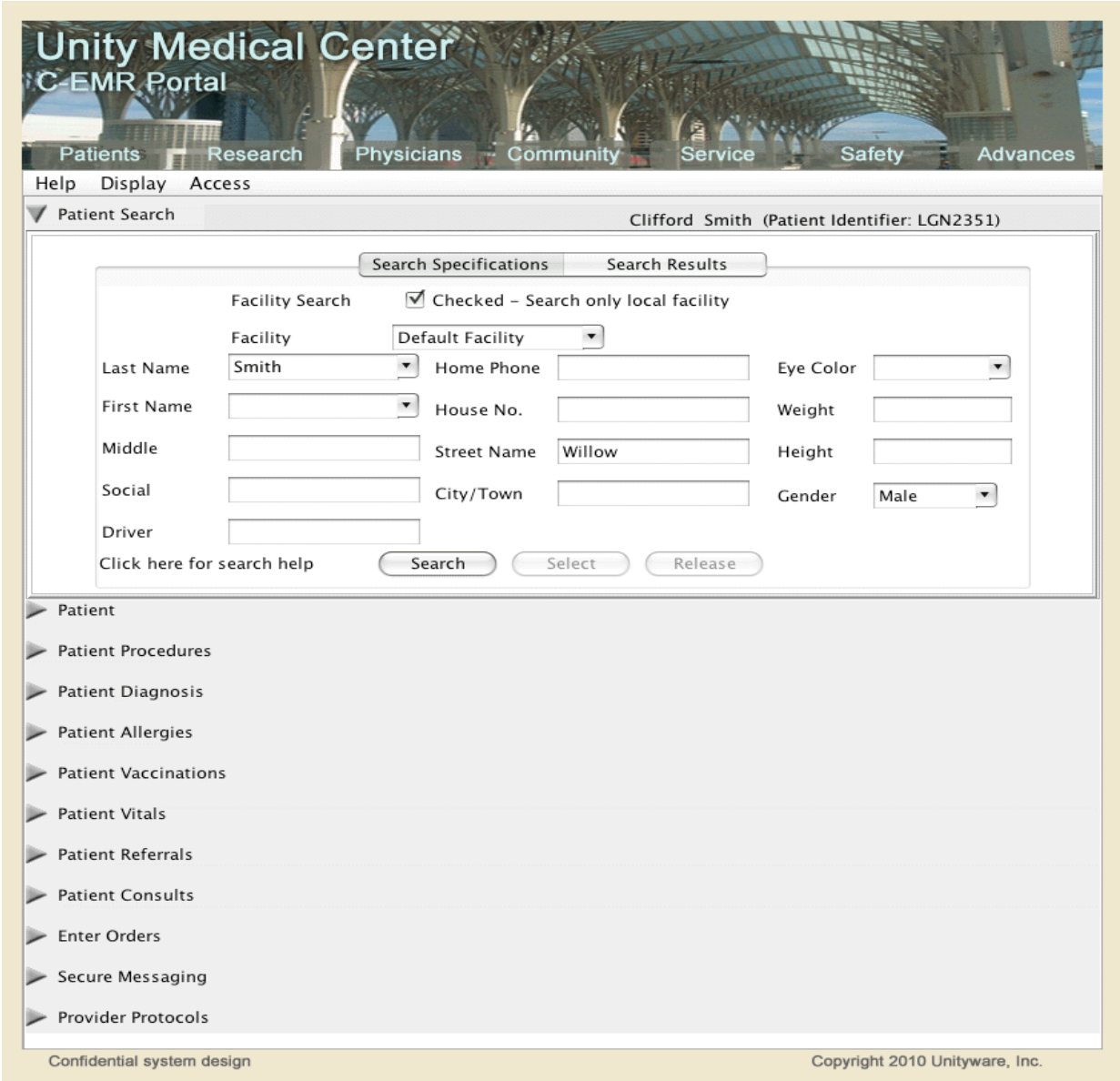
It might also be suggested that an incentive reimbursement plan be put in place, similar to the Federal ARRA EMR plan, for individual hospitals who buy or successfully develop a community-wide EMR system that can thereby be connected to the state HIE. This would greatly lower risk of failure and of loss of all moneys in that reimbursement would only be made after such systems were proven to meet minimum standards.

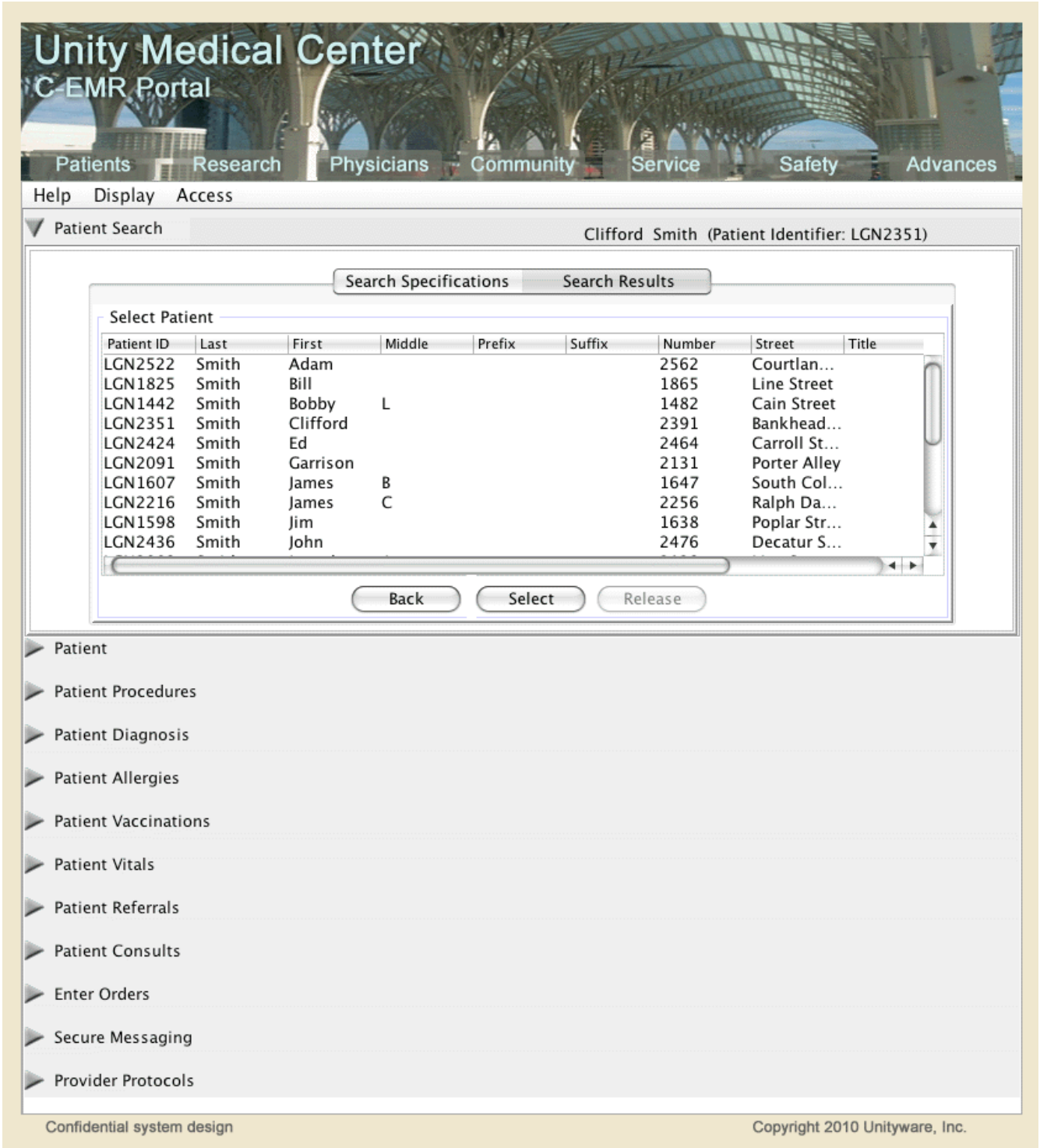
3. Direct Connection verses Portal Access

The SAGE-MR System has the ability to connect directly to any system, be it provider, payer, citizen, etc... However, this risks losing information. For example, if Hospital System-1 contains 30 fields of information and is sending straight into Hospital System-2, which only has 25 fields of information, then 5 pieces of information will be lost. That might be acceptable, but will have to be decided upon by the institution.

Therefore we present a duel solution in which we can connect systems or we can provided an interface (and perhaps feed the system from that). The interface will also be available for the provider that does not yet own an electronic system. This interface can be made available security for the Web.

This portal is totally customizable for the end user. A Heart Surgeon may well want his presentation of information to be different than a Podiatrist, a General Practitioner, ENT, Hospitalist or other doctor. It would certainly need to be different than what is seen by a billing clerk, admittance officer, etc... This portal allows that flexibility.




Unity Medical Center
C-EMR Portal
Patients
Research
Physicians
Community
Service
Safety
Advances
Help
Display
Access
Patient Search
Clifford Smith (Patient Identifier: LGN2351)
Search Specifications
Search Results
Select Patient
Patient ID | Last | First | Middle | Prefix | Suffix | Number | Street | Title
LGN2522 | Smith | Adam | | | | 2562 | Courtlan...
LGN1825 | Smith | Bill | | | | 1865 | Line Street
LGN1442 | Smith | Bobby | L | | | 1482 | Cain Street
LGN2351 | Smith | Clifford | | | | 2391 | Bankhead...
LGN2424 | Smith | Ed | | | | 2464 | Carroll St...
LGN2091 | Smith | Garrison | | | | 2131 | Porter Alley
LGN1607 | Smith | James | B | | | 1647 | South Col...
LGN2216 | Smith | James | C | | | 2256 | Ralph Da...
LGN1598 | Smith | Jim | | | | 1638 | Poplar Str...
LGN2436 | Smith | John | | | | 2476 | Decatur S...
Back
Select
Release
Patient
Patient Procedures
Patient Diagnosis
Patient Allergies
Patient Vaccinations
Patient Vitals
Patient Referrals
Patient Consults
Enter Orders
Secure Messaging
Provider Protocols
Confidential system design
Copyright 2010 Unityware, Inc.

4. Patient Recognition

The matching algorithm strategy is provided through a partner company. This partner has many years of consumer matching within the consumer marketing arena. This matching relies on a 'Knowledge Base' of billions of rows to effectively match individuals effectively and accurately. This knowledge base is feed daily with hundreds of sources of data including credit information, moves, warranty information, public records, property ownership information, marriage records, etc...

The matching algorithm relies on two key pieces of information. Those pieces are 1. Name and 2. Address. Given these two pieces of information, the system then 'cleans' the data and standardizes the information, specifically the address. It then does a string-based matching algorithm then bumps it against the historical knowledge base. After this is done, each person is assigned a UNIQUE alpha-numeric identifier. Over 94% of these people (based on average quality lists) also receive a PERSISTANT identifier. A persistent identifier basically means, 'The knowledge base has seen this person before.' They are likely a 'real' person. If the person has recently moved, their previous address can be used and that can create a lift of a percent or two.

Adding this knowledge based component normally increases matching by 10% or more over the best string-based matching algorithms. It can also do things that string based matching can't do, including:

1. Assign a persistent and unique identifier to an individual. This alpha-numeric identifier stays with them for life.
2. Allow the system to 'know' a person even if they have moved once or multiple times.
3. Allow the system to 'know' a person even if they have changed their name or go by variations of their name.

Example:

First	Last	Address	City	State	Zip	Dates	Unique and Persistent Identifier
Elizabeth	Wilson	123 Main St	Malvern	AR	72104	2001	XYZ123
Beth	Wilson	123 Main St	Malvern	AR	72104	2001	XYZ123
Elizabeth	Wilson	922 Orange Ln Apt 4483	Little Rock	AR	72211	2002	XYZ123
Elizabeth	Thomas	456 Beach Rd	Little Rock	AR	72211	2004	XYZ123
Elizabeth	Thomas	987 Pine Dr	Miami	FL	33114	2005	XYZ123
E.	Thomas	438 Park PL	Rogers	AR	72757	2008	XYZ123
Elizabeth	Thomas	88 Ridge St	Rogers	AR	72757	2008	JJJ999
Elizabeth	Thomas	776 Pebble Beach	Rogers	AR	72757	2010	XYZ123

Note the example above. Elizabeth (or Beth or E) Wilson started in Malvern in 2001, and was identified with XYZ123. She also used the name Beth. She then moved to a new address in 2002, but still was identified as the same person. In 2004 she married and changed her name to Thomas, but she was still correctly identified. In 2005 she and her husband moved out of state, yet her identifier remained constant. She went back to Arkansas in 2008 and still retained her unique and persistent identifier XYZ123. It seems that living near her was another Elizabeth Thomas at a different address, yet XYZ123 and JJJ999 remained unique and tied to their specific individual. Finally Elizabeth Thomas moved in 2010 and her identifier remained constant through this as well.

This unique and persistent identifier can be thought of as a sort of secure, generated, Social Security number, but without all the problems that go along with that. Also, there would be no way to 'steal' another person's identifier because it is a generated value that has no use unless the patient is there to receive services.

Using only name and address alone it is possible to correctly identify more than 92% of the people. It is very easy to add other criteria, such as SS #, date of birth, gender, drivers license number, etc... to bring the matching certainly to up over 99%.

Using this type of matching, it would be easy to match patients across multiple providers over time, even if the person has moved, changed their name, or gone out of state. Part of the beauty of this technology, is that it encompass the entire United States, and it can be used alone, or in conjunction with any other processes already in place.

Specifically, the matching process would work like this. All records would be matched across the Knowledge Based System and assigned the Unique and Persistent Identifier. These patients would have this identifier appended to their data where it would sit. Each time a patient sought treatment the providers system would communicate with the main system. In real time, that patient would be sent off to the Knowledge Based to have a persistent identifier appended. They would then use that identifier to link to the central system to determine if there is a match. If so, then that new information would be added and shared, bi-directionally, between the active provider and the historical super-system. If there was no match, then a new record would be created.

5. Provider Recognition

The way this is accomplished is to use National Provider Identifier within a table known as the Master Provider Directory. However, the flexibility of Unityware's system allows for other information to be carried and used as an alternate means of location. In addition, the Knowledge Base system described above for Individuals is also available for Business. As well Unityware's system could use Geo-Location, DUNS number, Department of Health (DOH) Licensing Database, or any other identifier that is needed.

Any reconsideration necessary between different providers would be accomplished automatically through the system through the use of a cross-reference lookup table. That is the beauty of the Unityware technology of uniting disparate systems. It would be doubtful that more than ½ an FTE would be needed to update tables. Their technology skills would need to be minimal and would be more clerical in nature.

The information stored on each provider would be standard such as Identification Numbers, Address, Phone Number, email address, etc... As well the system would/could store additional information such specialty, number of doctors, etc...

The problem with multiple physicians serving multiple locations would be handled by cross referencing tables and algorithms and rule sets that allow flexibility.
In order to be accurate, it would be wise to consider a cross reference between the Provider Identifier Database and the DOH in order to bubble up any discrepancies on a periodic basis. These could then be reconciled within the Master Provider Directory so that it always stays current.

6. Master Patient Index – How to Create an MPI from Disparate Systems

Unityware's new and proprietary Unityware interfaceless data unification technology will connect each disparate system to the super-system. "Interfaceless" is what we call our technology's ability to interface systems, but in a totally different manner than what is normally considered an interface. Unityware DOES NOT use traditional interfaces at the application layer to do this work. This is something completely new. In fact, a major, multi-national, independent, IT research firm has begun their initial paper on this technology. Their initial conclusion is that Unityware has created a NEW CATEGORY of technology. One which we feel is truly necessary to achieve a NHIN.
These disparate systems, connected by Unityware's interfaceless unification engine, can be clinics, hospitals, labs, payers, pharmacies, etc... The initial system will be linked together using the Unityware Server technology. Then, drawing from all sources of information the Patients will be linked together using a proprietary knowledge-base based individual matching algorithm. As Providers and their systems are added to the super-system they will be 'joined' to the system in the same way the initial Providers were.

Unityware's unique technology makes adding or changing sources of data highly scalable and not subject to the traditional problems of fragility when combining systems using various types of interfaces.

> Example: If Unityware combines 10 individual systems initially to create the super-system, it can easily add 10, 20, 200, 2,000 or more without affecting the super-system. Also if 2,000 systems are combined and system #25 (for example) needs to be changed in any way, there is no danger of the super-system being affected.

Unityware actually integrates systems by, first, isolating the entire database with a contextual buffer. Therefore, the traditional limitation on scalability and change are made moot because the contextual buffer automates the process of describing the raw data. Because the contextual buffer handles direct interrogation about the data in the system behind it, entire systems can be upgraded or replaced without affecting the rest of the environment. Unityware can be scaled from integrating just a few systems up to thousands. There is no theoretical limit.

Specifically, the Unityware Server (Unityware software running on a virtual or non-virtual server running Linux, Windows, Unix, etc..) will be connected to whatever other database system that exists and needs to be connected. The requirements will be that they need a direct, or VPN, connection to the system. Information such as IP Address, Port Number, User Name, and Password will be necessary to make the connection.

6. 1 How is data from disparate systems brought together in this solution?

The best technical approach to ensuring security, confidentiality, and integrity of patient records while accessing
them on a state-wide, or even national scale, is also one that happens to be entirely new.

Legacy role-based security mechanisms found within system applications today confine users to static r roles defined by rules in a system which better serve the system than the user. The dynamic and potentially emergent situations that frequently confront health care providers could not be more diametrically opposed to this. This results in such frequent use of "break-the-glass" overrides to traditional permission based systems that such static roles become meaningless. Health care is judicious and expeditious by nature and as such has led to the
invention of Unityware's Transportation of Authority security mechanism for patient information. Before this can be understood, the definition of the problem must be expanded upon: Most of the time spent working on software systems is spent solving problems caused by commitments to design philosophies in very early stages of development. Consider the answers to these questions:

*** Why are strict permissions and role definitions, to which such permissions must be attached, required in the first place?**

Answer: Because, due to early design philosophy, the data within the systems is browse-able within the system on a persistent basis thus access to data must be persistently restricted on a constant basis.

*** Why is the same data browse-able and "persistently available" within different systems in the first place?**

Answer: Because the data itself is being transported between systems before and instead of the authority to access the data.

*** Why is the data transported or "shared" in this way?**

Answer: Because conventional system security mechanisms are designed only to protect data within a system rather than a cloud of systems.

*** Doesn't this lead to complicated many-to-many, trust agreements between entities?**

Answer: Yes. Moreover, it is impossible to scale patient records only using traditional role-based permission security. This type of data security model first emerged as a way to protect files on a single computer and later a network of computers within an organization. When providing access to patient data on a national scale it is not realistic or practical to dictate consistently defined, let alone consistently enforced, role-based permission policies among thousands of health care provider entities. Thus something entirely new is required to be combined with such role based permissions.

The solution to all of this is best introduced using a practical example:

> A criminal needs to travel from New York to Chicago. He is early in his career in crime and can't afford to purchase his own plane ticket so being digitally savvy he decides on a high tech scam to travel for free. Our criminal likes the idea of stealing a boarding pass via an e-ticket kiosk because he can approach the unmanned device, print himself a free ticket, and get on his way to Chicago without drawing attention to himself.

> So on the day of his desired departure, our future convict arrives at the airport with stolen credit card in hand. He confidently approaches the kiosk, swipes his stolen card only to have the little screen report that no reservation exists for the victim, John Q Public. Not to be foiled so easily, he uses the screen pad to enter the name to search for reservations but alas still no reservation is found. So our baddie thinks, "No worries, I have this credit card. I'll just purchase a ticket, make the reservation, print the boarding pass, and be on my way." Ah but the e-ticket terminal is for check-in only. No way to make the reservation using the kiosk. Desperate, he approaches the counter, attempts to purchase a ticket from a live representative using the stolen credit card, is arrested and sent to prison. Our new convict now has plenty of time to contemplate the holes in his plan.

The point of this story is that data was well protected without role-based permissions. Actually, the reservation data is better protected at the kiosk than from a traditional computer terminal behind the desk because it is a non-browse-able point of access. To further the point, data is more easily protected when a corresponding event is required for the data to exist at a point of access. These events are a direct result of patron's activities rather than the volition of an "authorized" user of a system. Although there are many things that do not overlap between
this example and a patient receiving care within a health care community or various places throughout the US, it does depict an effective example of a Transportation of Authority. With this as the chosen model, the authority to access patient data follows the patient. Thus the patient data accessed exists as an event which is exactly what is happening in reality. Once the event is over, an x-ray is taken for example, the data retires to a historical resting place as part of the patient's health record, but no further authority to access that patient's data is offered or implied. Consider another illustration:

> You walk to your mailbox and open it. Among the contents is an invitation to a banquet. It contains the usual data: location, date, time etc. It even includes the name of the host. You attend the banquet and thoroughly enjoy the evening. You would like to send a gift to the host to express your appreciation and head to the post office. You arrive and present the postal clerk with your invitation and request the home address and telephone number for the banquet host. The expression on the clerk's face says it all but she gratuitously explains, "Sir, that's not how it works... You're supposed to know that already if you want to send something."

The point again is that the authority to attend one event implies no authority to attend another, nor can it be leveraged to access more data about the transporter of the authority. Moreover, the transportation system does not contain persistent, browse-able information. Thus securing data that does not exist is easy. Transportation of Authority keeps it confidential because only care providers who correspond to the patient care event can access the information. Further, the records are of the utmost integrity and quality because massive synchronization of traditionally shared data between systems is avoided entirely.

Connections to different health care systems already in place among provider entities can be handled this way: Unityware's data unification technology uses its synthetic intelligence to dynamically generate traditional interfaces with no programming. Specification for the interface are simply fed into the interface generator and the system builds the interface on its own without manual programming thus avoiding the FTE cost normally associated with this type of activity. Although the current capabilities obsolete the past patent: 6,864,779 the concept is similar.

Incoming data feeds do not need monitoring because data will not be moved from one system into another in the first place. This solves a significant problem regarding record authority that is not being considered by most designers of these systems. Since data is only transmitted during a patient care event, the parts of the health record that are not available from the original source will be flagged as such. This flag generates a support record that can automatically escalate to a support activity to investigate online/offline status of a system. However, a virtual copy of the clinical data for such a system can be used at the nearest point of presence within the community. In summary, combining the Transportation of Authority with the robust role-based security products from CA Inc data security is in very good hands.

6.2 How will this 'interface-less' technology be deployed?

The legacy interfacing technologies historically used in health care along with their modern permutations are the same ones which are landing best-of-breed provider systems in the dumpsters of hospitals all over the United States in favor of the now popular, and expensive, best-of-suite approach.

Maintaining rigid and subsequently fragile environments consisting of many heterogeneous systems connected via traditional interfacing methods has proven to be infeasible within the walls of many hospitals resulting in the rip-and-replace approach to achieving interoperability between departments; departments whom often capitulate superior best-of-breed functionality for the benefit to the hospital of having all departments using the same system so they can share information more economically. It seems unreasonable to expect such interfacing methods that cannot scale within the walls of a single hospital to be effective in building a flexible, robust, scalable, and highly available Health Information Network for the state of . An interfaceless data unification platform solves the aforementioned problems by connecting systems via contextual buffer technology from Unityware.

The contextual buffer is a synthetically intelligent layer which both automates the process of describing raw data within a clinical/hospital system and protects the FHIN from disruption caused by changes within hospital and clinic systems, wholesale replacement of systems, and decommissioning of such systems and/or entire provider facilities. It is this powerful and unique ability to automate the description of raw data within a system which makes this solution from Unityware the only realistic option to build a HIN which can support a complete longitudinal health record and also withstand the constant changes to systems in the theater without causing frequent outages to the FHIN. Because it is interfaceless, the implementation of this solution will require providers to purchase no expensive interfaces from their respective application system vendors nor endure the expense of divesting resources to long and complex programming projects typically associated with the implementation of such interface products. Because of its game changing architecture the implementation of the Unityware interfaceless data unification technology is done in a fraction of the time normally required by conventional methods. This makes the project completion more of a matter of logistics than waiting on **interfaces to be built.**

Unityware is backwardly compatible with legacy interfacing standards so that demarking the Arkansas HIE against the eventual National Health Network Connect System(s) will present no issues.

7. Security

Physical registration to the Arkansas Health Information Exchange (AHIE) would be managed by CA Identity Manager, which provides registration services, through a variety of mechanisms:

- Administrator Assisted: Identity Manager supports administrative registration, which could include pre-registration or partial registration. For example, a AHIE help desk administrator or a delegated administrator can create an initial account for a physician with some basic user profile information, and the physician could then be prompted to complete the registration form on initial login to the system.
- Self-Registration: An physician can register at the main AHIE portal/web site.
- Systematic: Identity Manager support automatic registration based on a feed from an authoritative source (e.g., HR system, Customer Care system, etc.). This would allow a hospital or medical group to automatically submit physician registrations to the AHIE. Similar to administrative registration, the systematic registration can also be partial, as the authoritative source may not contain all of the required profile attributes that the AHIE wants to capture.

In addition, the registration process can also trigger a work flow process that may require approvals prior to the account (or account changes) being made to the AHIE user store.

In terms of license validation, there are a variety of ways in which this could be implemented. For example, assuming that there is a registry of valid and/or invalid licenses, and this registry supports web service calls, CA Identity Manager could initiate a web service call during the registration process to this registry to determine if a physician has a valid license. Another approach would be to setup a work flow process whereby an administrator would "approve" a physician's registration request by manually/physically validating that the physician holds a valid license. The advantage to this approach is that the administrator could set an "end date" to the account, so that the physician's AHIE account (and access privileges) will expire when their license expires.

In terms of access permissions, the vast majority of AHIE users will interact with the system via the web portal interface. This interface was designed to support a Role-Based Access Control (RBAC) model. Therefore, when a user logs in, the application analyzes the roles assigned to the user and then displays only those tasks/activities that the user is allowed to perform. Similarly, when the user requests data, the system will retrieve only those patients records/data that the user is authorized to view/manage.

Although the RBAC model is defined within the AHIE solution, CA Identity Manager can automate the creation, modification, and deletion of user identities and their access to the AHIE resources. For example, when a new physician is registered, a basic account can be created within the AHIE application. Additional roles can then be assigned directly based on profile attributes, based on access request, or direct assignment by a delegated administrator. If required, CA Identity Manager can also initiate a workflow approval process for specific roles/access permissions. Finally, the system will audit all access permissions assigned to a physician for compliance audit and reporting purposes.

The AHIE Portal will be secured via CA SiteMinder.

CA SiteMinder is the most widely deployed Web Access Management (WAM) solution (over 1500 deployed customers) and proven platform (securing hundreds of thousands of applications worldwide) for addressing the challenges of today's Web-enabled enterprise. CA SiteMinder delivers:

- Shared authentication, authorization, and auditing services across the AHIE application components
- Unparalleled authentication approach and mechanism support
- The best performance and most scalable WAM solution available
- Enterprise-class administration and management features
- Technology leading features, such as policy analysis reporting and policy management
- An extensible architecture that simplifies upgrades

Because no single authentication technique is appropriate for all users, all access devices, and all protected resources in all situations, SiteMinder offers unparalleled control over what type of authentication method is used to protect a web resource and how that authentication method is deployed and managed. In addition, SiteMinder supports a range of authentication mechanisms.

Table : CA SiteMinder – List of Supported Authentication Methods.

Available Authentication Methods and Capabilities	
Anonymous Authentication	Microsoft Passport
Arcot Webfort (software two factor system)	One-time Passwords
Basic Authentication	RADIUS CHAP/PAP Authentication
Basic Authentication over SSL	RADIUS Server Authentication
Biometric Devices	Risk-based Authentication (via Arcot RiskFort)
CAPTCHA	RSA SecurID Authentication
CRYPTOCard RB-1	RSA SecurID Authentication with HTML Forms
Custom Authentication (via Authentication API)	SAML Tokens
Entrust IdentityGuard	SafeWord Server Authentication
HTML Forms	Smart Card
HTML Forms over SSL	TeleID Authentication
Information Card/Microsoft CardSpace	Third-Party Integrations: Tricipher, PassMark
Knowledge-based Authentication	X.509 Client Certificate
Login Sequence Control	X.509 Client Certificate and Basic
Machine Address Verification	X.509 Client Certificate or Basic
Microsoft ADFS	X.509 Client Certificate and HTML Forms
Microsoft Integrated Windows Authentication (IWA)	X.509 Client Certificate or HTML Forms
Microsoft NTLM/ADSA (supports MS Kerberos)	WS-Federation Tokens

In addition, SiteMinder supports the concept of protection levels, which are also commonly referred to as assurance levels. Each authentication method is associated with a specific protection level, ranging from 1 (lowest assurance level) to 1000 (highest assurance level). As web resources and/or applications are secured via SiteMinder security policies, a security administrator associates an authentication

method with a specific resource or group of resources. When a user attempts to access that resource, SiteMinder will ask four basic questions:

1. Is this resource protected?
2. Is this user authenticated?
3. Is this user authenticated at an equal or higher assurance level than the resource?
4. Is this user authorized?

The protection levels provide another layer of security within a single sign-on environment, namely, the ability to provide step-up security for specific resources and applications. When the user attempts to access one of these resources, SiteMinder will compare the protection level assigned to the resource against the protection level associated with the authentication credentials that the user presented at login. If the resource protection level is higher than the method used to authenticate the user, SiteMinder will prompt the user to enter a higher assurance credential. If the resource protection level is equal to or lower than the method used to authenticate, no re-authentication is required.

Finally, SiteMinder supports authentication alternatives via the Credentials Selector, which enables users to select the type of authentication credentials necessary to access protected resources. Based on the user's authentication context, the policy server will assign a specific protection level.

There are two basic approaches to connecting users accessing the AHIE with another HIE:

- Identity Federation
- Portal-based Web Services

In the first case, CA SiteMinder can support identity federation via an add-on module called CA SiteMinder Federation Manager (formerly CA SiteMinder Federation Security Services), which can extend the SiteMinder Single Sign-On (SSO) to external business partners federating into the AHIE (service provider model) and/or internal users federating to external web sites (identity provider model). CA SiteMinder Federation Manager provides federation through its support for the Security Assertion Markup Language (SAML), Microsoft ADFS, and WS-Federation.

In the second case, CA SiteMinder can also be integrated with CA SOA Security Manager to provide seamless SSO across web applications and web services, which provides significant value to organizations attempting to launch portal-based web services.

The following diagram illustrates a use case scenario that leverages this capability.

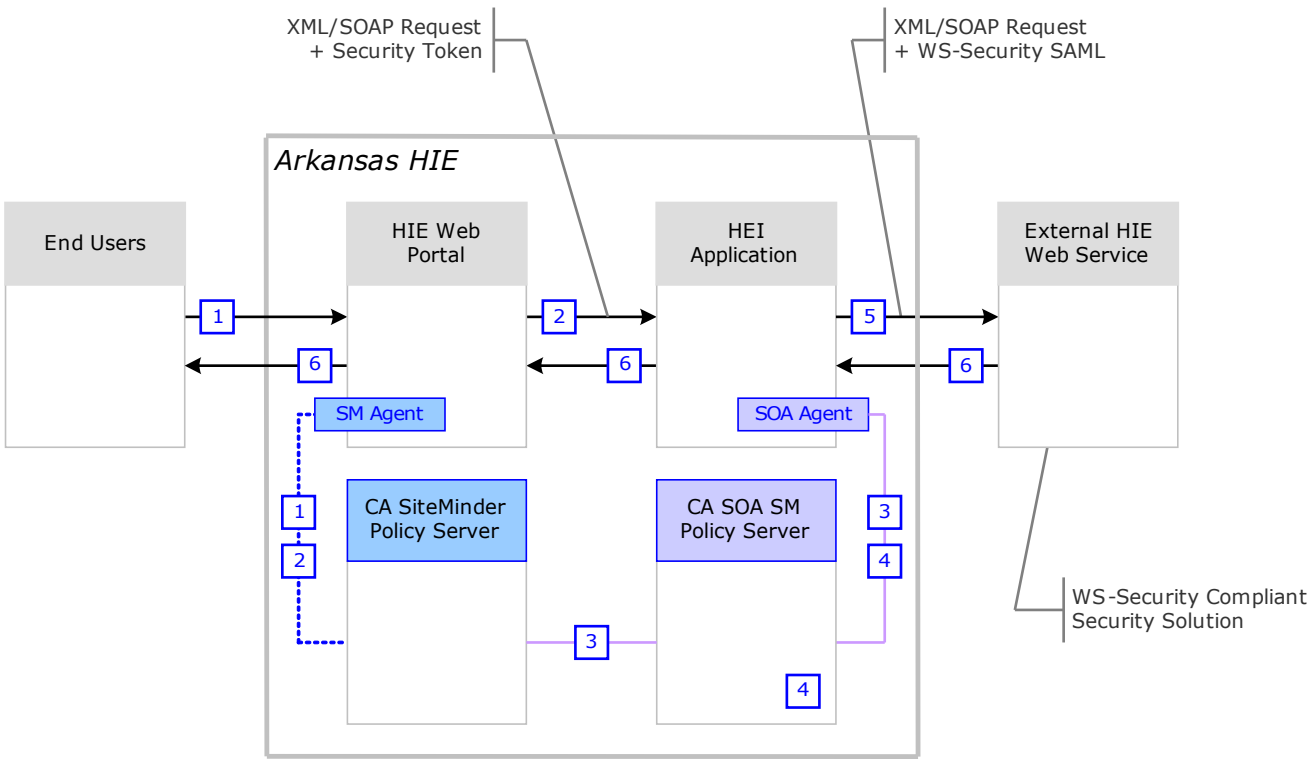


Figure : CA SiteMinder - SSO from Portal to Internal and External Web Services.

The process steps for this use case are as follows:

1. End user logs into the AHIE web portal, is authenticated by CA SiteMinder, and requests patient records that reside on an external HIE.
2. The FHEI portal-based application makes a SOAP call to internal patient record retrieval service using user's security context; which can be added via CA SiteMinder.
3. The user's session gets validated and authorized by the SOA Agent and CA SOA SM policy server, which is securing the patient record retrieval web service. The CA SOA SM policy server can validate the user's authentication though integration with CA SiteMinder.
4. CA SOA Security Manager generates a WS-Security/SAML token and adds it to SOAP Header of request for the next step in the web service — in this example to the retrieve a patient's record from an external HIE.
5. The AHIE patient record retrieval service sends SOAP request with SAML token to the external HEI.
6. The external HEI authenticates the web service request using WS-Security SAML standard and provides response to the FHEI patient record retrieval service, which in tern returns patient record data to the user on the portal-based application.

Role based permissions will be crucial to any medical system. Unityware can import these from existing systems and extend them accordingly.

First, since all 'touches' of patient data is tracked this can be tracked and reported to the individual patients similar to accessing a credit score or driving history is tracked and reported to the the individual. Patients could review their records and audit them making certain permitted access is occurring.

Secondly, certain patients are considered highly sensitive. This could be because of celebrity status or restraining order situations, etc... These patients could be protected by a flag in their record making it a requirement to gain two or more log-ons to see.

Another way to track access and allow 'break-the-glass' access in emergency situations is to tie the Unityware system in with the provider's admission system. For example: no one in a hospital could access a celebrity's records unless that person had been admitted through the ER or other channels. Therefore a curious person couldn't go surfing around looking for information unless they first admitted that patient to their clinic or hospital. Fraud could still be committed, but the burden associated with this would be very large and the person would certainly know they were being watched.

Finally, using such things as role based permission things would be secure on down the line. A celebrity patient might be admitted due to a car accident. Attending doctors would have access to his/her full records. They might order a series of x-rays. The radiology techs could look at that particular part of the patient's record, but not the entire thing and find out, for example, that the patient had once been treated for something they wished to remain private.

The SAGE-MR System will cover authorized access and permissions from end to end

The overall AHIE solution audits all user and site activity, including all authentications and authorizations, as well as administrative activity and any changes to the assigned access permissions and/or system configurations. Each individual component maintains its own audit store/log data; however, all of this data will be forwarded/collected by CA Enterprise Log Manager (CA ELM), which can provide comprehensive visibility of all IT activity within the AHIE system. CA ELM automates log collection, normalization and archiving across the entire AHIE, which not only reduces operational costs by eliminating inefficient, error prone procedures for log collection and compliance reporting, but also simplifies compliance auditing and forensic analysis.

Digital signatures can be used in different ways throughout the AHIE, including but not limited to:

- Web Browser to AHIE Interactions: SSL is supported between browser and web portal.
- Login Credentials: CA SiteMinder supports the use of X.509 client certificates as login credentials, and provides templates for the following certificate-based authentication schemes:
  - X.509 Client Certificates
  - X.509 Client Certificates and Basic
  - X.509 Client Certificates or Basic
  - X.509 Client Certificates and HTML Forms
  - X.509 Client Certificates or HTML Forms

    Client certificates can be software or hardware-based. In addition, it should be noted that CA SiteMinder has been deployed in several US Federal Agencies supporting the new HSPD-12 PIV Cards, which have been adopted by HiTrust.

- Internal Communications: CA SiteMinder and CA SOA Security Manager encrypt all data that is passed between its components. All traffic between the policy server, the web or SOA agents, the SOA gateway, and the admin interfaces is encrypted over TCP using 128-bit encryption (FIPS 140-2 certified) ; therefore, there is no use of HTTP or HTTPS through the firewall, providing very strong confidentiality of all information passed between these components.
- Web Services Communications: CA SOA Security Manager can provide message-level security via XML Signature, WS-Security encryption, and SAML.
- Log Data Communications: CA ELM uses SSLv3 for all transmission of log data between the agent and the server. This ensures that no one can eavesdrop and tamper logs in transit. This also ensures digital chain of custody. In addition, CA ELM Servers store logs in a binary format with read only access on the system. Also, the log data stored on external storage systems can be protected by using WORM (hardware or software) based storage solution.

CA offers several complimentary solutions that can be used to secure access to sensitive data beyond those already mentioned in this response, including:

- CA Access Control
- CA DLP

CA Access Control is designed to provide a comprehensive solution to privileged user management, protecting servers, applications and devices across platforms and operating systems. It provides a proactive approach to securing sensitive information and critical systems without impacting normal business and IT activities. CA Access Control helps to mitigate both internal and external risk by controlling how business or privileged users access and use enterprise data. The result is a higher level of security, a lower level of administrative costs, easier audit/compliance processes and a better user experience.

Key features of CA Access Control include:

- Role-based fine-grained access control
- Super user containment and rights delegation
- Server intrusion prevention
- UNIX Authentication Broker
- Dynamic policy management and automated distribution
- Self-protection mechanism
- Centralized & delegated administration
- Strong password management and policies, including privileged user passwords
- Privileged access auditing and entitlements reporting

The CA DLP solution includes a comprehensive and integrated set of products that help organizations manage the risk of uncontrolled information use and prevent data loss. The solution is a scalable, highly accurate and cost effective offering that is designed to protect and control data-in-motion on the network and in the messaging system, data-in-use at the endpoint, and data-at-rest on servers and in repositories across the enterprise. CA DLP provides a powerful solution that addresses all risks at a wide range of control points while leveraging a single infrastructure and platform.

CA DLP delivers a broad range of features to help your organization meet its data loss prevention and data protection goals:

- Complete Protection Coverage: Because of differing requirements and priorities, CA Data Loss Prevention protects data where needed — at the endpoint, message server, network, and for stored data.
- Identify Various Content Types: Customers have many data types that require protection. CA DLP can accommodate all of them — from personally identifiable information, to non-public information, to intellectual property.
- Accurate and Pre-Built Policies: With years of use and refinement in live customer deployments, CA DLP's pre-built policies leverage industry best practices for accurately identifying and protecting sensitive information. The accuracy techniques employed in our policies are unmatched.
- Appropriate Enforcement Actions: Using the right action is effective and efficient. There may be no need to involve management or dedicated reviewers when end-users can self-correct their own activity. Actions include block, warn, quarantine, redirect, move, delete, stub, capture and alert.
- Enterprise Scalability and Resilience: Deploy with confidence to thousands of desktops and scan terabytes of data. When connectivity to the central server is unavailable, the distributed components will continue to detect and protect data.
- Secure Review: Sensitive data is controlled during the review work flow, and is kept to reviewers with specific permissions and access.

8. Virtual Clinic

The SAGE-MR system makes use of a type of virtual clinic in order to centralize records into an MPI. This virtual clinic can be built and delivered in one of two ways, congruent with the desires of the committee.

8.1 Virtual Clinic – Non-Populated or Federated Model

In this version of the virtual clinic all data from all sources will be accessed. Records will be run through the linking process to append a unique and persistent identifier to them and a table will be created within the central host system with pointers to where all the various data sources for that individual exists.

In this version of the virtual clinic all the data would remain in the host systems. If they were off-line then no access could be gained to these records. However, this method gives more security to the central system as there would be no way to gain any information by breaching the host system. The information would strictly be unique ID and pointers.

8.2 Virtual Clinic – Populated or Hybrid Model

This design fulfills the requirement to create a hybrid model. Data would still stay in the individual host systems, and this data would be the most current possible. However, data would also be continuously backed up within the virtual clinic, just in case a system was down due to server failure, power outage, bandwidth disruption, etc...

The functionality would be such that a patient's record would be accessed by a provider. The pointers within the virtual clinic would direct the system to communicate with the networked systems in order to pull the latest information on that patient. If, however, one or more of the sources was off line, the fall back would be to the records stored in the virtual clinic. The provider would then be given a message saying something to this effect: “The system at Provider XYZ123 (Dr. Jones) is unavailable. More recent data may be contained there. This data is current though XX/XX/XX (example: some date from last week)” The provider could then ask the patient, “Have you seen Dr. Jones in the past week?” If not, then the provider WOULD have the most recent data. If not, then the provider would attempt to ask the patient or figure out if some critical information was missing and if so, what that information was.

The data within the virtual clinic would include, but not be limited to, the following information:

- Patient Demographics
  - Name
  - Address
  - Phone Number
  - Email Address
  - Date of Birth
  - SS #
  - Patient Identifier
  - Ethnicity
  - Gender
  - Insurance Type

    - Emergency Contact
    - Information Source Provider
    - Date of Information

- Vital Information
    - Height
    - Weight
    - BMI
    - Blood Pressure
    - Pulse
    - Smoking Status
    - Information Source Provider
    - Date of Information

- Health Issues
    - Current Diagnosis
    - Past Diagnosis
    - Procedures Performed
    - Information Source Provider
    - Date of Information
- Vital Encounter Information
    - Visit Type
    - Visit Date
    - Discharge Date
    - Procedures
    - Condition at Discharge
    - Date and Cause of Death (if applicable)
    - Information Source Provider
    - Date of Information
- List of Medications
    - Active List
    - Past History
- Diagnostic Test Results
    - Lab Reports
    - Pathology Reports
    - Radiology Reports
    - Cardiology Reports
    - Other Test Reports
    - Information Source Provider
    - Date of Information
- Physician Documentation
    - H&P
    - Progress Notes
    - Consulting Note
    - Operative Notes
    - Discharge Notes
    - Information Source Provider
    - Date of Information
- Images
- Reporting
    - Public Health Reporting
    - Quality Reporting
- Payer Information

- Immunizations
- Allergies
    - Drug Allergies
    - Food Allergies
    - Environmental Allergies

Also, it is important to note that the SAGE-MR system, using its portal could be extended to providers who do not have electronic systems, perhaps on a subscription fee basis. The providers, probably clinics more rural in nature, would be able to access the portal via a Web connection and use the Virtual Clinic as their EMR System as opposed to purchasing such a system from a vendor.

9. Reporting

9.1 Aggregate Reporting

Central to system is the ability for authorized persons to access data and run reports. These reports will be available in real time and allow researchers to design and build whatever reports they wish.

The system will have the ability to strip off such personally identifiable information as name, SS #, address, etc... and aggregate the data into reports.

Examples could include:

- Show the current number of H1N1 cases, by county for females over the age of 35.
- The number of non-smoking males between 21 – 30 who have been diagnosed and/or treated for lung cancer within the past two years.
- The numbers, by county, of people with a BMI over X% that suffer from heart disease.

These are just a few examples of the types of reports that could be run using linked data. These would only be limited by the imaginations of the researchers, who will now have access to, up until now undreamed of, amounts of quality real-time data.

The SAGE-MR System will support the use of such tools as Crystal Reports, Business Objects, etc...

9.2 Security Reporting

CA's suite of security products provide a wide range of security reports throughout the system. These reports are easily run through the CA products and can be use for audit purposes as well as fraud detection.

9.3 Usage Reporting

The Unityware System retains logs of every event within the system. Whenever records are modified, added, or even viewed a snapshot of that point in time is taken and stored. At any point in time records can be retrieved in order to show exactly what a provider or user saw. This is critical in order to defend against medical malpractice, and is standard within the system.

10. Payer Component

It is certainly within the realm of the SAGE-MR system to connect, bi-directionally, with any and all payers within the Medical Systems within the State.

These payers include any and all insurance companies as well as Medicare and Medicaid should they so wish to be linked.

The SAGE-MR system is envisioned to be one in which the Payers, provide claims information for their customers to be fed into the system for use within the MPI. This would fill a definite information hole within the system, especially if Arkansans have been provided treatment outside the State at providers not connected to the AHIE system, yet who filed claims with these Payers.

Some Payers are already providing a portal with claims information to the doctors. This is, of course, a very good thing. However, with patients being insured throughout their lives with different companies and since the doctors deal with multiple payers, it becomes very burdensome for the individual provider to look in a number of different places in order to piece together a history of their patients. For this reason, it is necessary that for these records to be fully utilized by the providers that they show up in one place, the MPI of the patient through the SAGE-MR system.

On the reverse end of the Payer Component it may/will be necessary to provide claims information to the various Payers. Although we do not have enough information at this time to make a complete proposal in this area, it is certainly well within the capability of the SAGE-MR system to facilitate claims processing, eligibility checking, etc...

Finally, a robust system of connected health data will have a tremendous benefit for the Payers in that they will be able to control some of the duplicate testing that goes on today because various providers are not able to see what other providers are doing.

11. Citizen Portal

A portal allowing individuals to access and even modify their medical records is a necessary component of a complete HIE. It is the position of the SAGE-MR system to support individual access to their own data, much in the same way they conduct on-line banking today or have access to their credit reports.

Citizens will wish to be able to log-in under a secure and verified account in order to check their records and perhaps even modify them. An example of this modification might be that they wish to have their records available, yet they wish to 'black list' some potentially embarrassing information. This could include:

- Mental Health Records
- Drug Overdose Procedures
- Venereal Diseases
- Substance Abuse Treatments
- Anything else that might potentially be embarrassing or highly private in nature

The one area that patients may not be able to have access to is physician notes. Physicians do no wish to 'have their hands tied' in writing notes if they know that one day their patients might read them. They might be far less likely to write truthfully ("this person is a hypochondriac" or "this person is probably faking his injury in order to get some pain pills") if this writing were to one day be subject to review by the patients who might wish to litigate.

Whatever data needs to be exposed or covered, it can be handled by the SAGE-MR System.

The security aspect of the patient portal is handled by CA SiteMinder, which is the most widely deployed Web Access Management (WAM) solution in the market (over 1500 deployed customers) and proven platform (securing hundreds of thousands of applications worldwide) for addressing the challenges of today's Web-enabled enterprise. CA SiteMinder Web Access Manager delivers:

Shared authentication, authorization, and auditing services across all web applications
Unparalleled user store and platform support
The best performance and most scalable WAM solution available
Enterprise-class administration and management features
Technology leading features, such as policy analysis reporting and policy management
An extensible architecture that simplifies upgrades

SiteMinder is the only solution that comprehensively addresses web site-management challenges and enables organizations to deploy e-business sites much more easily and cost-effectively -- and with greater security -- than any other technique or solution.

It is probably not the SAGE-MR System's intent to be the patient portal, but to instead feed that to the portal provider. There are a number of medical portal providers out there, including Google, who may wish to receive a feed of the SAGE-MR data in order to present it to the patients.

12. ProSys Professional Services

As one of the Southeast's largest reseller of information technology hardware and software systems integration and managed services providers, we offer the solution described to dramatically improve our clients' performance and health outcomes for citizens around the world. We leverage and apply our thought leadership, proven assets, talent and corporate citizenship agenda to identify and impact health-care's most pressing issues.

Our highly skilled professionals are trained not only to consult but to implement and manage your technology solutions as well, giving you the quality support you need from start to finish. In response to such demand Prosys has launched a Health & Public Service operating group to focus on and expand services to health care, government and public service clients.

ProSys technicians have years of hands-on experience and training under their belts. As a recognized information systems provider, we focus on finding the right solutions and making them work for you. To ensure that our solutions continue to serve our customers well, we offer various services and support options, from Lifecycle & Desktop Services to Integration & Distribution to full blown call center support. Ultimately, our goal is to improve the overall performance and operations of your organization through technology, leading to increased efficiency and productivity.

Implementation Services

Many will find that rolling out new technology solutions is frequently the most challenging aspect for an IT department due to the fact that poorly handled implementations often lead to reduced employee productivity and spiraling costs. ProSys understands this and that is why, through years of experience, we have demonstrated the expertise necessary to manage the business and process changes that come along with any IT implementation – large or small. ProSys uses solid project management methodologies and real-time, 24x7 communication to ensure that project time-lines are met and any unforeseen changes are properly managed.

Our implementation staff is specially trained not only to handle the toughest challenges, but also to work directly with our clients throughout the process. We keep you and your staff informed regarding project status as well as notifying you of any possible issues or concerns, should they arise. Our flexible, conscious approach enables us to reduce risk and control costs, helping you implement flawless procedures to ensure quality on-time implementations.

Our implementation services include:

- Project Management
- On-Site Installation
- Data Migration
- User-Level Customization
- Training
- Real-Time Project Status Reporting

13. Hardware Requirements

13.1 Solution Requirements

The SAGE-MR system will have a minimum amount of hardware associated with it. Within the State HIE the requirements for Unityware are as follows.

- A modern server running either Unix, Linux, Windows, or Mac.
- CPU—Single or dual-processor, Intel Pentium III (or compatible), 700-900 MHZ.
- Memory—512 MB system RAM. We recommend 1 GB.
- Available disk space—540 MB.
- Temp directory space—450 MB.
- The Server can be virtualized.

The CA solution will run on a variety of platforms as well and will require less than 4 actual servers of similar requirements to the Unityware Server above. Virtualization may be a possibility as well.

The solution also will require ongoing storage capacity, probably via a SAN, in order to store the data.

* The requirements above do not include backup, fail-over, or disaster recovery hardware.

13.2 Networking Requirements

The SAGE-MR system assumes that network components be in place at both the core and the end points. This can be accomplished through a secure WAN or through VPN connections.

The SAGE-MR system does not include VPN devices or Routers, however they can be secured through ProSys.

14. High Level Features and Benefits

The features and benefits of the SAGE-MR system are great and can be found throughout this document. However, we wished to create a simple section in which people could gain a high-level overview without having to dig through this long document. Also, this section is easily sharable.

SAGE-MR connects with any provider. We can connect all providers regardless of what system they are using at their hospital, clinic, pharmacy, state agency, etc.. Unityware is completely agnostic in terms of who it can link. *It is simple for Unityware to connect to any software.*

SAGE-MR provides 96% + positive patient identity. In partnership with another company, we can match patients using a knowledge-based system that relies on 6 billion rows of historical data. This system assigns a unique and persistent identifier to every patient. It is unique to each individual and persistently follows them as they move and even if they change their names. Therefore no medical records are lost as people's lives change.

No record left behind. SAGE-MR can retrieve and load legacy information from one system to another so that no records are left behind.

SAGE-MR solution is secure and highly available -- built from the ground up using industry leading CA technologies.

The SAGE-MR solution contains multiple levels of security. The system can be easily set to treat specific records differently, such as in the case of celebrity or domestic abuse restraining order cases. The data can also be easily made accessible based upon user permissions. Therefore private medical information would be hidden from the billing clerk, and Psychological or other sensitive can be excluded based on need-to-know requirements.

The SAGE-MR system can be changed in a fraction of the time of other systems. Our technology provides that changes can be made to the system in far less time than any previous system. If a major change needs to be made, an *authorized* user can make that change. If it is of a larger nature then the response time and resultant costs are a fraction of what would normally be expected. With Unityware, days become hours, weeks become days, months become a week or two.

"Catch a thief." The SAGE-MR system makes it very easy to catch 'frequent fliers' or others who wish to scam the medical system in search of narcotics or other illegal or false activities.

Stay in Sync. With the SAGE-MR design, medical information does not get out of sync as with traditional amalgamation architecture and does not have the security exposure of traditional federated designs.

Improve Patient ID protection. The SAGE-MR solution can allow patients to be authenticated before entering them into a provider's system. This prevents fraud, for example, should one patient try to falsely use another patient's insurance.

Reduce lawsuit costs. The SAGE-MR solution captures 'snap shots' each and every time patient information is accessed. This, frozen in time, snapshot gives providers protection as to exactly what a professional saw during a given instant for use in medical malpractice cases.

Access is not limited to ..... The SAGE-MR system can not only be used by providers with disparate systems, but also by providers without an EMR. Unityware can provide access to a 'virtual clinic' of information through a web browser interface.

Advanced search and graphics reporting formats easily available. The SAGE-MR System can provide multiple types of robust reporting to the providers. The SAGE-MR system can provide the information in many ways through advanced searching and even graphically.

The SAGE-MR System provides robust research capabilities. We can strip off personally

identifiable information and provide robust research capabilities through reporting both textually and graphically using advanced search techniques.

Example: A researcher might want to find the percentage of patients in 68 of Arkansas' counties (but not the other 7) who are between the ages of 48 and 62 who have had a heart attack in the past 3 years, but who do not smoke.

This type of research could be available in minutes.

The SAGE-MR results at a fraction of the cost. Comparatively, far far less expensive than any competition that can even claim to achieve the same results.

The SAGE-MR Unifies but also isolates.....What??? Unityware is a revolutionary tool for unifying systems, but it also isolates those systems from changes that occur in other changes. Using traditional methods it is possible to link multiple systems together. However, a change in System-A can cause a cascading problem and bring down System-D, System-F, and System-R. Unityware eliminates that, so changes or upgrades can be made without ever recoding or testing the interfaces.

The SAGE-MR System Scales – Grow the system from one entity to hundreds or thousand without leaving behind any technology.

15. Solution Provider Credentials

CA Overview

CA has been helping companies manage Information Technology (IT) in all kinds of environments for more than three decades. From the mainframe to distributed to virtualized and cloud, we have a history of developing and delivering powerful, integrated software to help customers improve performance and better compete, innovate and grow their businesses. We have grown from a four-person operation in the mid-1970s to a global IT management software company that today serves the majority of the Forbes Global 2000. In addition, FORTUNE recently announced that CA has been ranked #482 on the 2010 FORTUNE 500 list; CA climbed 47 spots from last year and moved into the #4 position on FORTUNE's Computer Software list.

CA's Security Management product portfolio provides a complete and comprehensive solution to meet the most critical security needs of IT organizations today. This suite of products provides a unique set of advantages including: comprehensive reach across large, heterogeneous environments, broad capabilities to help secure all IT resources, product-level integration for easier and consistent administration across all of IT, and proven scalability to meet the needs of the largest and most complex IT environments. In addition, CA Security Management products are modular solutions and can be deployed individually, or in combination with products from other vendors, to meet organization's unique needs. As a fundamental function of supporting management of enterprise IT infrastructure, CA's Security Management solutions help monitor and protect user access, automate security processes, and achieve compliance easier throughout the entire organization.

The conceptual building blocks of the CA Security Management are shown in the diagram below.

Figure: CA Security Management Solution Context.

There are three key things that you need to control for effective security and compliance: user identities, their access, and their use of information. CA's Content Aware IAM is different from other vendors because it provides an integrated solution to control all of these areas.

Traditional IAM stops at the point of access, so organizations have less control of their information and identities. No other security vendor has the complete product portfolio required to deliver CA's Content Aware IAM.

To help you achieve even better overall security, our longer-term strategy is to further automate security controls by dynamically adjusting policies based on intelligence gained from user access and information activity. For example, if someone has access rights to certain information but never uses it, maybe that access privilege should be removed. Or, if certain information is deemed to be possibly misused, the access policy can be dynamically changed to eliminate that access privilege from the user. These innovative capabilities will serve to further establish CA's uniqueness among IAM vendors.

Unityware Overview

Unityware is a tech start up, founded upon a legacy of other successes within the medical field. Unityware's founder, Brian Stack, has a long track record of success. He has founded two profitable companies, one of which he took public. The other he venture funded after it was profitable. This company secured medical luminaries as clients including, IVAX and Beckman/Coulter.

His team has been developing the Unityware technology over the past 9 years, creating an incredible new type of computer technology that obsoletes all of their past patents. Unityware's current technology, is being sold and implemented in hospitals and medical clinics today. The company is headquartered in Arkansas, and can be found on the Web at www.unityware.com

Unityware is an Arkansas founded and based company. The company is currently housed as the first 'Business in Residence' at the University of Arkansas at Little Rock School of Business. Unityware is also supported by Innovate Arkansas and The Arkansas Science and Technology Authority (ASTA).

ProSys Overview

Originally founded in 1997 and based in Atlanta, GA, ProSys was created to deliver customized IT solutions backed by comprehensive engineering expertise and best-in-class products. Today, employing approximately 350 people with a near 3:1 ratio of Senior Consultants to Account Executives, we continue to work hard to be your trusted IT advisor.

ProSys serves mid-market, enterprise, public sector and educational organizations. We assess, design, acquire, implement and support IT hardware and software solutions for our clients. Our goals are to help our clients minimize their cost structure, increase the effectiveness of their supply chain, secure their network, improve communications and develop a customized storage management solution.

Our physical office locations are found primarily in the southeastern region of the United States; however, ProSys offers deployment services, delivery capabilities and more throughout the US. ProSys has resources of far-reaching channel agreements, as well as both national and international service and delivery options, allowing us to deploy resources quickly and efficiently. This flexibility helps us ensure that our customers are receiving the information and resources they need to deal with all of their IT and business challenges.

What we do:

ProSys successfully brings together customized IT solutions and comprehensive engineering expertise, coupled with proprietary technology applications and best-in-class products to offer solutions tailored to meet your organization’s unique business requirements. We assess, design, acquire, implement and support your IT hardware and software solutions.

16. Currently Installed Locations

The beginnings of the SAGE-MR system are currently installed at Arkansas Methodist Medical Center in Paragould Arkansas. As well, Unityware has completed a successful proof of concept on this technology at Saline Memorial Hospital in Benton Arkansas.

More prospects throughout the State and Nation are being added weekly.

17. Estimated Costs and Time-line

This is obviously a very difficult area to nail down at this time. However, a broad estimation can be given, based upon known factors. This estimation includes both the cost of the SAGE-MR solution at the state level as well as the estimated cost of the solution at the local level. This local cost would have to be multiplied out by the number of hospitals who wish to connect their hospital to their community of clinics (see Section 2).

Also, this estimation does not include cost of networking equipment, bandwidth, or state employees. However, due to the highly automated nature of this system the number of supporting state employees would be minimal. It is estimated that it would take no more than 3 or 4 FTE's to maintain all levels of service for this system. Also, there may well need to be some sort of call center set up for support.

State HIE Costs (Parallel Phase A)*

These costs include the central system and the license to connect it to 100 other systems. Installation Services represent a block of time sufficient for ProSys to do the installation with these systems.

• Initial Software Cost	$ 5,000,000
• Installation Services	1,000,000
• Annual Software Maintenance	1,000,000
• Hardware	15,000
Total Year One -	$ 7,015,000

Local CEMR Costs (Parallel Phase B) *

Community Electronic Medial Records system installed in local hospitals and reaching out to local clinics. These CEMR systems, available through ProSys, benefit the local hospitals and doctors in these ways. The CEMR solution includes connections and services to install up to 30 clinical systems.

- Outpatient Computerized Provider Order Entry Systems (CPOE)
- Inpatient CPOE
- Clinic to Clinic Referrals
- Access to Patient Medical Records by Other Clinicians and Hospitalists.

• Initial Software Cost	$ 250,000
• Installation Services	50,000
• Annual Software Maintenance	50,000
• Hardware	5,000
Total Year One -	$ 305,000

- As part of the SAGE-MR proposal, we will include software and installation for 4 CEMR systems. In other words, a value of $ 1,220,00. These sites can be chosen by the State HIE Committee or they can use to reapportion the money in the form of incentive payments to spread this money to multiple hospitals.

Time-Line

The time-line of what it would take to implement is, of course, very nebulous. Much of it would depend upon how eager various hospitals, providers, payers, etc... we willing and able to connect. Assuming there would be little delays in this a time-line might look something like this.

State Level

- Contract awarded and paperwork completed (Day One)
- State HIE installed and connected to 20 entities (3 Months)
- Connections to 30 more entities (4 months)
- Connections to 30 more entities (3 months)
- Connections to 20 more entities (2 months)

Local Level (this is already being done by this system).

- Contract awarded and paperwork completed (Day One)
- Hospital connection installed for hospital to clinics and Hospital to State HIE (1 month)
- Connections to 30 clinics (2 months)

18. Glossary

AHIE – Arkansas HIE or Health Information Exchange.

Aggregate – Pull together data from different systems/sources.

ARRA – American Recovery and Reinvestment Act. ARRA mandates that providers adopt 'meaningful use' of Electronic Medical Records by 2015 in order to avoid a Medicare/Medicaid Penalty Phase. There is an incentive phase from 2011 – 2014.

CA- Formerly known as Computer Associates, CA is a Fortune 500 software company specializing in IT Security solutions. www.ca.com

CEMR – Community Electronic Medical Record (Includes local hospital and local clinics.

Clinic – On office housing one or more doctors. These can be General Practitioners or Specialist.

EHR – Electronic Health Record (same as EMR).

EMR – Electronic Medical Record.

HIE – Health Information Exchange.

HIS – Health Information System. These are used within hospitals or clinics and are supplied by a number of vendors such as, but not limited to, McKesson, Epic, Medatech, eClinical Works, Siemens, CPSI, etc...

Hospitalist – A type of doctor that does not have a private practice, but works solely for a hospital. Since Hospitalists do not have easy access to a patient's medical history the ability to access them quickly, accurately, and electronically is critical.

MPI – Master Patient Index – This is an amalgamation of all the available health information on a given patient. Since patients tend to be treated, over time, by multiple providers then this information most often must come from multiple sources.

Meaningful Use – Minimum functionality standards set by the Federal Government governing the ability to create and use Electronic Medical Records.

NHIN – National Health Information Network.

Payer – A Payer is any entity that processes medical claims and is responsible for paying them. These can include all types of health insurance companies as well as Medicare and Medicaid.

PCP – Primary Car Physician.

PHR – Personal Health Record. An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual.

ProSys – ProSys is a Value Added Reseller (VAR) of all types of hardware and software solutions. www.ProSysis.com

Provider – Any individual doctor, dentist, clinic, hospital, pharmacy, laboratory, or other entity that provides medical care or related services.

RHIO – Regional Health Information Organization.

SAGE-MR- The solution presented by ProSys and delivered by Unityware and CA.

SHARE - State Health Alliance for Records Exchange

Unityware – Unityware is an Arkansas based software company specializing in linking disparate systems and data together using a revolutionary new technology. www.unityware.com